

Formation certifiante Les technologies de sécurité en environnement Microsoft Azure

Durée de la formation : 9 jour(s) / 63 heure(s)

OBJECTIFS

A l'issue de la formation le participant sera capable de :

- Concevoir une stratégie d'instrumentation DevOps
- Mettre en oeuvre des processus de développement DevOps
- Mettre en oeuvre un processus d'intégration continue
- Mettre en oeuvre un processus de livraison continue
- Implémenter la gestion des dépendances
- Mettre en oeuvre l'infrastructure d'application
- Mettre en oeuvre un processus de feedback continu
- Se préparer et passer les examens :

- AZ-900 : Concepts de base de Microsoft Azure
- AZ-104 : Administrateur Microsoft Azure
- AZ-500 : Associé Ingénieur en Sécurité Azure

PREREQUIS

Connaissances attendues : Azure (Azure-AD, VNet, NSG, Key Vault, stockage, VMs...), sécurité cloud, identités et accès

Compétences de base : Cryptographie, authentification, pare-feux, DDoS, VPN, conformité cloud

Langue technique : Anglais professionnel souhaité

Un entretien en amont avec notre expert permet de prendre en compte le profil de chaque participant (niveau, objectifs et résultats attendus, contexte professionnel, enjeux...) et d'adapter le contenu de la formation si besoin. Cette formation ne peut être financée que dans le cadre d'un projet d'entreprise (prise en charge entreprise ou OPCO). Les dossiers à financement personnel et CPF ne sont pas pris en compte.

PUBLIC

Administrateurs Azure souhaitant apprendre à sécuriser, surveiller et gérer les ressources sur Azure

Professionnels IT / ingénieurs sécurité cloud impliqués dans la mise en œuvre de contrôles de sécurité sur Azure

Architectes cloud qui veulent renforcer la sécurité de leurs infrastructures Azure

Développeurs, responsables conformité ou équipes IT en charge de la gouvernance et sécurité sur Azure

Formation certifiante Les technologies de sécurité en environnement Microsoft Azure

Durée de la formation : 9 jour(s) / 63 heure(s)

PROGRAMME

Identité

Azure Active Directory
Utilisateurs et Groupes
Laboratoire : Gérer les Identités d'Azure Active Directory
Après avoir terminé ce module, les étudiants seront capables de:
Sécuriser et gérer les identités avec Azure Active Directory.
Mettre en œuvre et gérer les utilisateurs et les groupes.

Gouvernance et Conformité

Abonnements et Comptes
Azure Policy
Contrôle d'Accès en Fonction du Rôle (RBAC)
Laboratoire : Gérer les Abonnements et RBAC.
Laboratoire : Gérer la Gouvernance par le biais d'Azure Policy.
Après avoir terminé ce module, les étudiants seront capables de:
Mettre en œuvre et gérer des abonnements et des comptes Azure.
Mettre en œuvre Azure Policy, ce qui inclut les politiques personnalisées.
Utiliser RBAC pour attribuer des autorisations.

Administration d'Azure

Azure Resource Manager
Azure Administrator Tools
Modèles ARM
Laboratoire : Gérer les ressources Azure en utilisant des modèles ARM
Laboratoire : Gérer les ressources Azure en utilisant Azure PowerShell (facultatif)
Laboratoire : Gérer les ressources Azure en utilisant Azure CLI (facultatif)
Laboratoire : Gérer les ressources Azure en utilisant le Azure Portal
Après avoir terminé ce module, les étudiants seront capables de:
Tirer parti d'Azure Resource Manager pour organiser les ressources.
Utiliser Azure Portal et Cloud Shell.
Utiliser Azure PowerShell et CLI.
Utiliser les ARM Templates pour déployer les ressources.

Mise en Réseau Virtuelle

Réseaux Virtuels.
Groupes de Sécurité du Réseau.
Azure Firewall.
Azure DNS.
Laboratoire : Mise en œuvre d'un réseau virtuel.
Après avoir terminé ce module, les étudiants seront capables de:
Mettre en œuvre des réseaux et des sous-réseaux virtuels.
Configurer des groupes de sécurité du réseau.
Configurer l'Azure Firewall.
Configurer les zones DNS privées et publiques.

Formation certifiante Les technologies de sécurité en environnement Microsoft Azure

Durée de la formation : 9 jour(s) / 63 heure(s)

Connectivité intersites

VNet Peering.

Connexions de passerelles VPN.

ExpressRoute et WAN virtuel.

Laboratoire : Mise en œuvre de la connectivité intersites.

Après avoir terminé ce module, les étudiants seront capables de:

Connecter VNet Peering.

Configurer les passerelles VPN.

Choisir la solution de connectivité intersites adéquate.

Gestion du Trafic du Réseau

Routage du réseau et des points de terminaison.

Azure Load Balancer.

Azure Application Gateway.

Laboratoire: Mise en œuvre de la Gestion du Trafic.

Après avoir terminé ce module, les étudiants seront capables de:

Configurer le routage du réseau, ce qui inclut les routes personnalisées et les points de terminaison des services.

Configurer un Azure Load Balancer.

Configurer une Azure Application Gateway.

Stockage Azure

Comptes de Stockage.

Stockage des Blobs.

Sécurité du Stockage.

Fichiers Azure et File Sync.

Gestion du Stockage.

Laboratoire : Gérer le Stockage Azure.

Après avoir terminé ce module, les étudiants seront capables de:

Créer des comptes de stockage Azure.

Configurer des conteneurs de blobs.

Sécuriser le stockage Azure.

Configurer les fichiers Azure et File Sync.

Gérer le stockage avec des outils tels que Storage Explorer.

Machines Virtuelles Azure

Planification des Machines Virtuelles.

Création des Machines Virtuelles.

Disponibilité des Machines Virtuelles.

Extensions des Machines Virtuelles.

Laboratoire : Gérer les Machines Virtuelles.

Après avoir terminé ce module, les étudiants seront capables de:

Planifier la mise en œuvre des machines virtuelles.

Créer des machines virtuelles.

Configurer la disponibilité des machines virtuelles, ce qui inclut les ensembles de mise à l'échelle.

Utiliser les extensions des machines virtuelles.

Formation certifiante Les technologies de sécurité en environnement Microsoft Azure

Durée de la formation : 9 jour(s) / 63 heure(s)

Informatique Sans Serveur

Azure App Service Plans

Azure App Service

Container Services

Azure Kubernetes Service

Laboratoire : Mise en œuvre des applications Web.

Laboratoire : Mise en œuvre du Azure Kubernetes Service

Laboratoire : Mise en œuvre des Azure Container Instances

Après avoir terminé ce module, les étudiants seront capables de:

Créer un plan de service pour une application.

Créer une application Web.

Mettre en œuvre Azure Container Instances.

Mettre en œuvre le service Kubernetes d'Azure.

Protection des données

Sauvegarde des Fichiers et Dossiers.

Sauvegarde des Machines Virtuelles.

Laboratoire : Mettre en œuvre de la Protection des Données.

Après avoir terminé ce module, les étudiants seront capables de:

Sauvegarder et récupérer des fichiers et des dossiers.

Sauvegarder et récupérer des machines virtuelles.

Surveillance

Azure Monitor

Azure Alerts

Log Analytics

Network Watcher

Laboratoire : Mise en œuvre de la Surveillance

Après avoir terminé ce module, les étudiants seront capables de:

Utiliser Azure Monitor.

Créer des alertes Azure.

Effectuer des requêtes à l'aide de Log Analytics.

Utiliser Network Watcher.

Gestion des Identité et accès

Configurer Azure Active Directory pour les charges de travail Azure workloads et les abonnements

Configurer Azure AD Privileged Identity Management

Configurer la sécurité pour les abonnements Azure

Protection de la plate-forme

Comprendre la sécurité cloud

Créer un réseau

Sécuriser le réseau

Mettre en place la sécurité des hôtes

Implémenter la sécurité de la plateforme

Implémenter la sécurité des abonnements

Formation certifiante Les technologies de sécurité en environnement Microsoft Azure

Durée de la formation : 9 jour(s) / 63 heure(s)

Opérations de sécurité

- Configurer les services de sécurité
- Configurer des stratégies de sécurité à l'aide d'Azure Security Center
- Gérer les alertes de sécurité
- Répondre aux problèmes de sécurité et les corriger
- Create security baselines

Données et applications

- Configurer des stratégies de sécurité pour gérer les données
- Configurer la sécurité pour l'infrastructure de données
- Configurer le chiffrement pour les données at rest
- Comprendre la sécurité des applications
- Implémenter la sécurité pour le cycle de vie des applications
- Sécuriser les applications
- Configurer et gérer Azure Key Vault

Travaux pratiques

- Contrôle d'accès basé sur les rôles
- Politique Azure
- Verrous du Resource Manager
- MFA, accès conditionnel et protection de l'identité AAD
- Gestion des identités privilégiées d'Azure AD
- Mise en oeuvre de la synchronisation des répertoires
- Groupes de sécurité réseau et groupes de sécurité des applications
- Pare-feu Azure
- Configuration et sécurisation de l'ACR et de l'AKS
- Key Vault (mise en oeuvre de la sécurisation des données par la configuration de Always Encrypted)

Formation certifiante Les technologies de sécurité en environnement Microsoft Azure

Durée de la formation : 9 jour(s) / 63 heure(s)

Prise en compte du handicap

Pour les personnes en situation de handicap, afin de nous permettre d'organiser le déroulement de la formation dans les meilleures conditions possibles, contactez-nous via notre formulaire de contact ou par mail (formation@access-it.fr) ou par téléphone (0320619506). Un entretien avec notre référente handicap pourra être programmé afin d'identifier les besoins et aménagements nécessaires.

Modalités et moyens Pédagogiques, techniques et d'encadrement mis en œuvre

Répartition théorie/pratique : 45%/55%. Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques s'articulant autour d'une application fil rouge, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.

Formation accessible à distance de n'importe où et n'importe quand, via un ordinateur type PC disposant d'une connexion à Internet à haut débit (ADSL ou plus).

Pour assurer un démarrage dans les meilleures conditions au premier jour de la formation, notre service logistique se met systématiquement en relation, en amont, avec vous afin de réaliser un test de validation technique et de vous présenter l'environnement de formation.

Pendant toute la durée de la formation, le stagiaire dispose d'une assistance technique et pédagogique illimitée, par e-mail, avec un délai de prise en compte et de traitement qui n'excède pas 24h. En complément, le stagiaire peut planifier un rendez-vous pédagogique avec un formateur expert afin d'échanger sur des éléments de la formation.

La durée de la formation affichée sur cette page est une durée estimée qui peut varier en fonction du profil du stagiaire et de ses objectifs (notamment s'il souhaite valider sa formation par le passage d'un examen de certification).

Durant la formation, le formateur prévoit :

Des démonstrations organisées en modules et en séquences découpées le plus finement possible, en suivant le programme pédagogique détaillé sur cette page ;

Des énoncés et corrigés de travaux pratiques à réaliser tout au long de la formation ;

Des travaux pratiques sont proposés ; la plateforme prévoit l'environnement technique nécessaire à la réalisation de l'ensemble des travaux pratiques ;

Le formateur valide les connaissances acquises après chaque TP ;

Il est proposé un ou plusieurs livres numériques faisant office d'ouvrage(s) de référence sur le thème de la formation.

Validation et sanction de la formation

Une attestation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation sera remise au stagiaire à l'issue de sa formation par courrier électronique.

A la demande, il sera délivré un certificat de réalisation.

Type de formation

Professionalisante ayant pour objectif le perfectionnement, l'élargissement des compétences

Moyens permettant de suivre l'exécution de l'action

Le contrôle de la présence des stagiaires sera assuré par la vérification de l'assiduité des participants. Le stagiaire signera une feuille de présence par demi-journée de formation. Celle-ci sera également signée par le formateur.

Modalité d'évaluation des acquis

Durant la formation, le participant est amené à mettre en pratique les éléments du cours par la réalisation de travaux pratiques réalisés sur PC.

La validation des acquis du stagiaire est faite par le formateur à la fin de chaque atelier. Cette validation individuelle est possible du fait du faible nombre de participants par session de formation (6 personnes maximum).

À la fin de la formation, le stagiaire a donc atteint les objectifs fixés par la formation.

En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par l'éditeur en passant un examen de certification.

Access it étant centre d'examen ENI, les examens peuvent être réalisés sur demande à distance ou dans nos locaux de Villeneuve d'Ascq.

Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification

Assistance Post-Formation

Toute personne ayant suivi une formation avec Access it bénéficie d'une assistance post-formation d'une durée de 1 mois. Ce nouveau service d'accompagnement permet aux stagiaires rencontrant des difficultés dans la mise en œuvre des connaissances acquises de solliciter l'aide de nos formateurs sur des aspects relatifs aux programmes de formation suivis. Pour en bénéficier, il suffit de se rendre sur la page contact de notre site web et de remplir le formulaire. Une réponse est apportée par mail ou par téléphone dans un délai de 48 heures.

Centre d'Examen

Notre centre de formation agréé Qualiopi bénéficie de l'agrément d'ENI et ICDL pour les certifications informatiques. C'est pour nos clients la garantie de pouvoir suivre des formations préparant à des certifications professionnelles.

Aide à l'orientation

Pour chacune des grandes thématiques couvertes par notre offre de formation, nous proposons via nos spécialistes un rendez-vous physique ou téléphonique qui via un diagnostic permettra aux personnes souhaitant être accompagnées dans le choix d'un programme ou dans la définition d'un parcours de formation une orientation vers les programmes les plus adaptés à leurs besoins et à leur niveau.

Aspects Pratiques

Dès leur inscription, les participants sont contactés par nos services qui s'assurent que les débits internet constatés sur le lieu depuis lequel ils souhaitent se former sont suffisants pour suivre la formation dans des conditions optimales.

À l'occasion de cet appel, nos experts s'assurent également qu'ils disposent du matériel nécessaire pour suivre la formation (PC Portable, webcam, Micro-casque..).

Avant le début de la formation, les participants reçoivent un lien leur permettant d'accéder à la classe virtuelle et leurs identifiants personnels de connexion. Un aide à l'utilisation de la solution de visioconférence utilisée leur est également proposée.

Le jour de la formation, ils se connectent à la classe virtuelle depuis leur navigateur internet. Ils voient et entendent le formateur ainsi que les autres participants et peuvent à tout moment communiquer avec eux.

Ils participent aux échanges et réalisent les ateliers dans les mêmes conditions que s'ils étaient en salle. Grâce à nos outils de prise en main à distance, les formateurs peuvent à tout moment prendre la main sur leurs postes pour les aider ou vérifier leurs TP.

Tout au long de la formation, les participants peuvent bénéficier de l'assistance immédiate de nos experts en composant le numéro qui leur a été communiqué avant la formation.

Des bilans intermédiaires ont lieu en présence des participants du formateur et du référent pédagogique d'Access it afin de vérifier l'état d'avancement de la session, les difficultés rencontrées et permettre d'éventuels actions correctives.

Bénéfices pour les participants

Se former depuis leur lieu de travail ou leur domicile,

Accéder sans se déplacer à la qualité d'une formation délivrée par un formateur consultant ayant une expérience probante sur le sujet animé.

Bénéficier à distance de la richesse d'une formation interentreprises : échanges avec le formateur et les autres participants, partages d'expériences, ateliers pratiques...

Pouvoir se former en toutes circonstances et notamment en cas d'imprévu.

Bénéfices pour l'entreprise

Optimiser ses budgets en limitant les frais de déplacement et d'hébergement.

Proposer à tous ses collaborateurs, quelle que soit leur situation géographique, des formations de qualité (en Inter comme en Intra).

Limites les temps de déplacement.

Proposer davantage de choix dans les formations à des collaborateurs peu mobiles.

Assurer la montée en compétences de ses collaborateurs quelles que soient les circonstances